

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-282803

(43)Date of publication of application : 15.10.1999

(51)Int.CI.

**G06F 15/00**

(21)Application number : 10-081789      (71)Applicant : MITSUBISHI ELECTRIC CORP

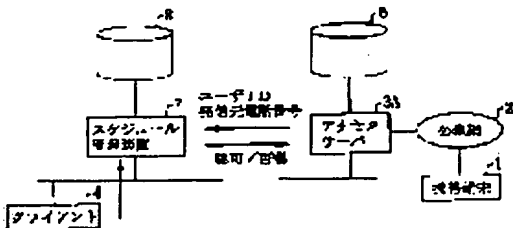
(22)Date of filing : 27.03.1998 (72)Inventor : ARAKI TOSHIO  
SHIMIZU MICHIO  
KATO ATSUSHI  
SAITO TAKUMA  
MATSUHIRA KEIICHI

**(54) ILLEGAL ACCESS PREVENTION SYSTEM**

**(57)Abstract:**

**PROBLEM TO BE SOLVED:** To double decide the propriety of connection and accordingly to improve the security.

**SOLUTION:** A schedule management device 7 receives a user ID and the telephone number of an originator from a server 3A, compares the received telephone number with the telephone number of the originator previously registered and informs the server 3A of the comparison result. Receiving the comparison result from the device 7, the server 3A notifies a portable terminal of the permission and rejection of access when coincidence and no coincidence are confirmed between both telephone numbers of the originator respectively.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other  
than the examiner's decision of rejection or  
application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's  
decision of rejection]

[Date of requesting appeal against  
examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(書誌+要約+請求の範囲)

---

(19)【発行国】日本国特許庁(JP)

(12)【公報種別】公開特許公報(A)

(11)【公開番号】特開平11-282803

(43)【公開日】平成11年(1999)10月15日

(54)【発明の名称】不正アクセス防止システム

(51)【国際特許分類第6版】

G06F 15/00 330

【FI】

G06F 15/00 330 B

【審査請求】未請求

【請求項の数】5

【出願形態】OL

【全頁数】14

(21)【出願番号】特願平10-81789

(22)【出願日】平成10年(1998)3月27日

(71)【出願人】

【識別番号】000006013

【氏名又は名称】三菱電機株式会社

【住所又は居所】東京都千代田区丸の内二丁目2番3号

(72)【発明者】

【氏名】荒木 敏夫

【住所又は居所】東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72)【発明者】

【氏名】清水 道夫

【住所又は居所】東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72)【発明者】

【氏名】加藤 敦史

【住所又は居所】東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72)【発明者】

【氏名】齋藤 琢磨

【住所又は居所】東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72)【発明者】

【氏名】松比良 啓一

【住所又は居所】東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(74)【代理人】

【弁理士】

【氏名又は名称】曾我 道照（外6名）

---

(57)【要約】

【課題】 従来の不正アクセス防止システムでは、パスワードが第三者に漏れる可能性があるという課題があった。

【解決手段】 アクセスサーバ3 AからユーザID及び発信元電話番号を受け取り前記発信元電話番号と予め登録された発信元電話番号と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置7を備え、アクセスサーバ3 Aは、前記スケジュール管理装置から前記比較結果を受け取り前記発信元電話番号同士が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知する。

【効果】 2重に接続可否を判定することになり、セキュリティの強化を図ることができる。

---

【特許請求の範囲】

【請求項1】 携帯端末からアクセス要求があった場合には前記携帯端末からユーザID及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザID及び第1のユーザ識別情報を受け取り前記第1のユーザ識別情報とスケジュールテーブルに予め登録された第2のユーザ識別情報と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザID、パスワード及び第1のユーザ識別情報を受け取り前記ユーザID及びパスワードと登録内容と比較して一致したときは前記ユーザID及び第1のユーザ識別情報を前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記比較結果を受け取り前記第1及び第2のユーザ識別情報が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知することを特徴とする不正アクセス防止システム。

【請求項2】 携帯端末からアクセス要求があった場合には前記携帯端末からユーザID及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末

に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザIDを受け取り前記ユーザIDに基づきスケジュールテーブルから予め登録された第2のユーザ識別情報を読み出して前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザID、パスワード及び第1のユーザ識別情報を受け取り前記ユーザID及びパスワードと登録内容と比較して一致したときは前記ユーザIDを前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記第2のユーザ識別情報を受け取り前記第1及び第2のユーザ識別情報が一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知することを特徴とする不正アクセス防止システム。

【請求項3】 前記第1及び第2のユーザ識別情報は、前記携帯端末の発信元電話番号であることを特徴とする請求項1又は2記載の不正アクセス防止システム。

【請求項4】 前記第1のユーザ識別情報は、前記携帯端末の位置情報であり、前記第2のユーザ識別情報は、前記登録された位置情報であることを特徴とする請求項1又は2記載の不正アクセス防止システム。

【請求項5】 前記第1のユーザ識別情報は、前記携帯端末の発信元電話番号及び位置情報であり、前記第2のユーザ識別情報は、前記携帯端末の発信元電話番号及び前記登録された位置情報であることを特徴とする請求項1又は2記載の不正アクセス防止システム。

## 詳細な説明

---

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 この発明は、企業などの組織内ネットワークへの公衆網を介したアクセスにおいて、第三者からの不正なアクセスを防止する不正アクセス防止システムに関するものである。

【0002】

【従来の技術】 従来の不正アクセス防止システムについて図面を参照しながら説明する。  
図19は、従来の不正アクセス防止システムの構成を示す図である。

【0003】 図19において、1は携帯端末、2は公衆網、3は組織内ネットワークのアクセスサーバ、4は組織内ネットワークのクライアント、5は組織内ネットワークのサーバである。

【0004】 携帯端末1から公衆網2経由で組織内ネットワークへ接続し、内部のコンピュータを利用する場合、組織内ネットワークへ接続する際に、正規のユーザからの接続要求であるか否かを判定し、セキュリティを確保する必要がある。このセキュリティ確保は、

組織内ネットワークのアクセスサーバ3でアクセスの制御を行うことにより達成されている。

【0005】図19に示すように、あらかじめ組織内ネットワークへのアクセスが許可されたユーザ毎に、「ユーザID」と、「パスワード」とを設定する。アクセスサーバ3は、アクセス開始時にユーザIDとパスワードをユーザに要求し、許可されているユーザIDとパスワードが一致したときに、組織内ネットワークへのアクセスを許可する。

【0006】

【発明が解決しようとする課題】 上述したような従来の不正アクセス防止システムでは、パスワードが第三者に漏れる可能性があり、それを悪用して組織内ネットワークへ接続される恐れがあるという問題点があった。

【0007】この発明は、前述した問題点を解決するためになされたもので、組織外にある端末から公衆網経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置とアクセスサーバを連携させ、ユーザID、パスワード、発信電話機の番号、個人の行動に合わせた接続可否を判定することにより、セキュリティの強化を図ることができる不正アクセス防止システムを得ることを目的とする。

【0008】

【課題を解決するための手段】 この発明に係る不正アクセス防止システムは、携帯端末からアクセス要求があった場合には前記携帯端末からユーザID及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザID及び第1のユーザ識別情報を受け取り前記第1のユーザ識別情報とスケジュールテーブルに予め登録された第2のユーザ識別情報と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザID、パスワード及び第1のユーザ識別情報を受け取り前記ユーザID及びパスワードと登録内容と比較して一致したときは前記ユーザID及び第1のユーザ識別情報を前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記比較結果を受け取り前記第1及び第2のユーザ識別情報が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知するものである。

【0009】この発明に係る不正アクセス防止システムは、携帯端末からアクセス要求があった場合には前記携帯端末からユーザID及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザIDを受け取り前記ユーザIDに基づきスケジュールテーブルから予め登録された第2のユーザ識別情報を読み出して前記アクセスサーバ

に通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザID、パスワード及び第1のユーザ識別情報を受け取り前記ユーザID及びパスワードと登録内容と比較して一致したときは前記ユーザIDを前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記第2のユーザ識別情報を受け取り前記第1及び第2のユーザ識別情報が一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するものである。

【0010】また、この発明に係る不正アクセス防止システムは、前記第1及び第2のユーザ識別情報を、前記携帯端末の発信元電話番号としたものである。

【0011】また、この発明に係る不正アクセス防止システムは、前記第1のユーザ識別情報を、前記携帯端末の位置情報とし、前記第2のユーザ識別情報を、前記登録された位置情報としたものである。

【0012】さらに、この発明に係る不正アクセス防止システムは、前記第1のユーザ識別情報を、前記携帯端末の発信元電話番号及び位置情報とし、前記第2のユーザ識別情報を、前記携帯端末の発信元電話番号及び前記登録された位置情報としたものである。

【0013】

【発明の実施の形態】実施の形態1. この発明の実施の形態1に係る不正アクセス防止システムについて図面を参照しながら説明する。図1は、この発明の実施の形態1に係る不正アクセス防止システムの構成を示す図である。なお、各図中、同一符号は同一又は相当部分を示す。

【0014】図1において、1は携帯端末、2は公衆網、3Aは組織内ネットワークのアクセスサーバ、4は組織内ネットワークのクライアント、6はユーザ毎のユーザIDとパスワードが登録されているファイル装置、7は組織内ネットワークのスケジュール管理装置、8は個人のスケジュールテーブルが登録されているファイル装置である。

【0015】図2は、この発明の実施の形態1に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【0016】図2に示すように、スケジュールテーブルは、ユーザ（個人）毎に構成され、さらに、ユーザー一人について「ユーザ番号」と、「ユーザID」と、時間に対応した「滞在場所」と、同様に時間に対応した「発信元電話番号であるアクセス権」とから構成されている。

【0017】つぎに、この実施の形態1に係る不正アクセス防止システムの動作について図面を参照しながら説明する。図3及び図5は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図4は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【0018】ユーザは、図2に示すように、行動スケジュールの各項目、すなわち、スケジュールテーブルの「ユーザID」と、一日の時間に対応した「滞在場所」及び「アクセ

ス権（発信元電話番号）」をスケジュール管理装置7を介してファイル装置8に登録しておく。スケジュールテーブルで、アクセス権を「禁止」にした時間中は、公衆網2からのアクセスを禁止する。一方、スケジュールテーブルのアクセス権に「電話番号」に登録すると、その電話番号からの発信についてのみ公衆網2からのアクセスを許可する。

【0019】上述したように、ユーザは、予めスケジュール管理ツールに行動スケジュールに登録しておく。そして、アクセスサーバ3Aは、公衆網2からの接続要求を受けたとき、携帯端末1で使用している電話番号（発信元電話番号）を公衆網2から受けとる。この時、「ユーザID」と「発信元電話番号」をスケジュール管理ツールへ渡す。

【0020】スケジュール管理ツールでは、受けた「ユーザID」に対応した行動スケジュールを検索し、当該電話番号からのアクセスを許可している時間帯かどうかを判定し、アクセスサーバ3Aへ結果を返す。

【0021】アクセスサーバ3Aは、スケジュール管理ツールの判定結果が「認可」であれば、携帯端末1と組織内ネットワーク間の接続（通信）を、携帯端末1からの切断要求を受けるまで保持し、判定結果が「否認」であれば、直ちに通信を切断する。

【0022】すなわち、図3のステップ10において、アクセスサーバ3Aは、携帯端末1からアクセス要求を受け付ける。

【0023】次に、ステップ11において、アクセスサーバ3Aは、携帯端末1から、「ユーザID」と、「パスワード」と、「発信元電話番号」を受け取る。

【0024】次に、ステップ12において、受け取った「ユーザID」及び「パスワード」を、ファイル装置6に登録されているユーザID及びパスワードと比較する。

【0025】次に、ステップ13～14において、携帯端末1から受け取った「ユーザID」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ3Aは「ユーザID」及び「発信元電話番号」をスケジュール管理装置7に送る。

【0026】ステップ15～16において、アクセスサーバ3Aは、携帯端末1から受け取った「ユーザID」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末1に通知し、携帯端末1との接続を断つ。

【0027】つづいて、図4のステップ20において、スケジュール管理装置7は、「ユーザID」及び「発信元電話番号」をアクセスサーバ3Aから受け取る。

【0028】次に、ステップ21～22において、スケジュール管理装置7は、組織内ネットワーク内の時計から日時を読み込み、「ユーザID」と現在の時間に基づきファイル装置8内のスケジュールテーブルを検索し、登録された発信元電話番号を読み出す。

【0029】次に、ステップ23において、アクセスサーバ3Aから受け取った「発信元電話番号」を、ファイル装置8から読み出した発信元電話番号と比較する。

【0030】次に、ステップ24～25において、アクセスサーバ3Aから受け取った「発信元電話番号」と登録内容が一致した場合は、スケジュール管理装置7はアクセス認可をアクセスサーバ3Aに通知する。



【0031】ステップ26において、スケジュール管理装置7は、アクセスサーバ3Aから受け取った「発信元電話番号」と登録内容が一致しなかった場合には、アクセス否認をアクセスサーバ3Aに通知する。

【0032】つづいて、図5のステップ30において、アクセスサーバ3Aは、アクセス可否判定結果をスケジュール管理装置7から受け取る。

【0033】次に、ステップ31～33において、スケジュール管理装置7からアクセス認可を受け取った場合は、アクセスサーバ3Aはアクセス許可を携帯端末1に通知し、組織内ネットワークとの通信を許可する。

【0034】ステップ34～35において、アクセスサーバ3Aは、スケジュール管理装置7からアクセス否認を受け取った場合には、アクセス拒否を携帯端末1に通知し、携帯端末1との接続を断つ。

【0035】この実施の形態1に係る不正アクセス防止システムは、組織外にある端末1から公衆網2経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置7とアクセスサーバ3Aを連携させ、ユーザID及びパスワードと、携帯端末1Aの電話番号とに基づき2重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【0036】実施の形態2. この発明の実施の形態2に係る不正アクセス防止システムについて図面を参照しながら説明する。上記の実施の形態1ではスケジュール管理装置7で発信元電話番号を登録内容と比較しアクセス可否を判定していたが、この実施の形態2ではアクセスサーバ3Bがアクセス可否の判定を行う。

【0037】なお、この実施の形態2に係る不正アクセス防止システムの構成は、上記の実施の形態1とほぼ同様であるので図示を省略する。但し、アクセスサーバ及びスケジュール管理装置の符号を3B及び7Aとする。

【0038】図6及び図8は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図7は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【0039】図6のステップ40において、アクセスサーバ3Bは、携帯端末1からアクセス要求を受け付ける。

【0040】次に、ステップ41において、アクセスサーバ3Bは、携帯端末1から、「ユーザID」と、「パスワード」と、「発信元電話番号」を受け取る。

【0041】次に、ステップ42において、受け取った「ユーザID」及び「パスワード」を、ファイル装置6に登録されているユーザID及びパスワードと比較する。

【0042】次に、ステップ43～44において、携帯端末1から受け取った「ユーザID」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ3Bは「ユーザID」をスケジュール管理装置7Aに送る。

【0043】ステップ45～46において、アクセスサーバ3Bは、携帯端末1から受け

取った「ユーザID」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末1に通知し、携帯端末1との接続を断つ。

【0044】 つづいて、図7のステップ50において、スケジュール管理装置7Aは、「ユーザID」をアクセスサーバ3Bから受け取る。

【0045】 次に、ステップ51～52において、スケジュール管理装置7Aは、組織内ネットワーク内の時計から日時を読み込み、「ユーザID」と現在の時間に基づきファイル装置8内のスケジュールテーブルを検索し、登録された発信元電話番号等のアクセス権データを読み出す。

【0046】 次に、ステップ53において、スケジュール管理装置7Aは、読み出したアクセス権データをアクセスサーバ3Bに通知する。

【0047】 つづいて、図8のステップ60において、アクセスサーバ3Bは、アクセス権データをスケジュール管理装置7Aから受け取る。

【0048】 次に、ステップ61において、アクセスサーバ3Bは、携帯端末1から受け取った「発信元電話番号」とアクセス権データの内容である発信元電話番号が一致した場合は、アクセス認可と判定する。一方、携帯端末1から受け取った「発信元電話番号」とアクセス権データの内容である発信元電話番号が一致しなかった場合には、アクセス否認と判定する。さらに、アクセスサーバ3Bは、アクセス権データの内容が禁止である場合はアクセス否認と判定する。

【0049】 次に、ステップ62～64において、アクセス認可と判定した場合は、アクセスサーバ3Bはアクセス許可を携帯端末1に通知し、組織内ネットワークとの通信を許可する。

【0050】 ステップ65～66において、アクセスサーバ3Bは、アクセス否認と判定した場合には、アクセス拒否を携帯端末1に通知し、携帯端末1との接続を断つ。

【0051】 この実施の形態2に係る不正アクセス防止システムは、組織外にある端末1から公衆網2経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置7Aとアクセスサーバ3Bを連携させ、ユーザID及びパスワードと、携帯端末1の電話番号とに基づき2重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【0052】 実施の形態3. この発明の実施の形態3に係る不正アクセス防止システムについて図面を参照しながら説明する。図9は、この発明の実施の形態3に係る不正アクセス防止システムの構成を示す図である。

【0053】 図9において、1AはGPS機能を有する携帯端末、2は公衆網、3Cは組織内ネットワークのアクセスサーバ、4は組織内ネットワークのクライアント、6はユーザ毎のユーザIDとパスワードが登録されているファイル装置、7Bは組織内ネットワークのスケジュール管理装置、8は個人のスケジュールテーブルが登録されているファイル装置である。

【0054】図10は、この発明の実施の形態3に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【0055】図10に示すように、スケジュールテーブルは、ユーザ（個人）毎に構成され、さらに、ユーザー一人について「ユーザ番号」と、「ユーザID」と、時間に対応した「滞在場所」と、同様に時間に対応した「住所（位置情報）」とから構成されている。

【0056】つぎに、この実施の形態3に係る不正アクセス防止システムの動作について図面を参照しながら説明する。図11及び図13は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図12は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【0057】図10に示すように、ユーザは、行動スケジュールの各項目、すなわち、スケジュールテーブルの「ユーザID」と、一日の時間に対応した「滞在場所」及び「住所（位置情報）」をスケジュール管理装置7Bを介してファイル装置8に登録しておく。

【0058】上述したように、ユーザは予めスケジュール管理ツールに行動スケジュールを登録しておき、また、GPS機能を備えた携帯端末1Aを持つ。そして、アクセスサーバ3Cは、公衆網2からの接続要求を受けた時、GPS機能により認識された「位置情報」を受け取り、「ユーザID」と「位置情報」をスケジュール管理ツールへ渡す。

【0059】スケジュール管理ツールでは、受けた「ユーザID」に対応した行動スケジュールを検索し、当該位置情報に対応する地域からのアクセスを許可している時間帯かどうかを判定し、アクセスサーバ3Cへ判定結果を返す。この場合の位置情報は、誤差が発生する可能性があるので、必要に応じてアクセスを許可する地域に余裕を持たせる。

【0060】アクセスサーバ3Cでは、スケジュール管理ツールの判定結果が認可であれば携帯端末1Aと組織内ネットワーク間の接続（通信）を、携帯端末1Aからの切断要求を受けるまで保持し、判定結果が否認であれば直ちに通信を切断する。

【0061】すなわち、図11のステップ70において、アクセスサーバ3Cは、携帯端末1Aからアクセス要求を受け付ける。

【0062】次に、ステップ71において、アクセスサーバ3Cは、携帯端末1Aから、「ユーザID」と、「パスワード」と、「位置情報」を受け取る。

【0063】次に、ステップ72において、受け取った「ユーザID」及び「パスワード」を、ファイル装置6に登録されているユーザID及びパスワードと比較する。

【0064】次に、ステップ73～74において、携帯端末1Aから受け取った「ユーザID」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ3Cは「ユーザID」及び「位置情報」をスケジュール管理装置7Bに送る。

【0065】ステップ75～76において、アクセスサーバ3Cは、携帯端末1Aから受け取った「ユーザID」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末1Aに通知し、携帯端末1Aとの接続を断つ。

【0066】つづいて、図12のステップ80において、スケジュール管理装置7Bは、「ユ

ーザID」及び「位置情報」をアクセスサーバ3Cから受け取る。

【0067】次に、ステップ81～82において、スケジュール管理装置7Bは、組織内ネットワーク内の時計から日時を読み込み、「ユーザID」と現在の時間に基づきファイル装置8内のスケジュールテーブルを検索し、登録された位置情報を読み出す。

【0068】次に、ステップ83において、アクセスサーバ3Cから受け取った「位置情報」を、ファイル装置8から読み出した位置情報と比較する。

【0069】次に、ステップ84～85において、アクセスサーバ3Cから受け取った「位置情報」と登録内容が一致した場合は、スケジュール管理装置7Bはアクセス認可をアクセスサーバ3Cに通知する。

【0070】ステップ86において、スケジュール管理装置7Bは、アクセスサーバ3Cから受け取った「位置情報」と登録内容が一致しなかった場合には、アクセス否認をアクセスサーバ3Cに通知する。

【0071】つづいて、図13のステップ90において、アクセスサーバ3Cは、アクセス可否判定結果をスケジュール管理装置7Bから受け取る。

【0072】次に、ステップ91～93において、スケジュール管理装置7Bからアクセス認可を受け取った場合は、アクセスサーバ3Cはアクセス許可を携帯端末1Aに通知し、組織内ネットワークとの通信を許可する。

【0073】ステップ94～95において、アクセスサーバ3Cは、スケジュール管理装置7Bからアクセス否認を受け取った場合には、アクセス拒否を携帯端末1Aに通知し、携帯端末1Aとの接続を断つ。

【0074】この実施の形態3に係る不正アクセス防止システムは、組織外にある端末1Aから公衆網2経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置7Bとアクセスサーバ3Cを連携させ、ユーザID及びパスワードと、携帯端末1Aの位置情報とに基づき2重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【0075】実施の形態4. この発明の実施の形態4に係る不正アクセス防止システムについて説明する。上記の実施の形態3ではスケジュール管理装置7Bで位置情報を登録内容と比較しアクセス可否を判定していたが、この実施の形態4ではアクセスサーバ3Dがアクセス可否の判定を行うものである。

【0076】なお、この実施の形態4に係る不正アクセス防止システムの構成は、上記の実施の形態3とほぼ同様であるので図示を省略する。但し、アクセスサーバ及びスケジュール管理装置の符号を3D及び7Cとする。

【0077】また、この実施の形態4に係る不正アクセス防止システムの動作は、図6～図8に示す実施の形態2のアクセスサーバ及びスケジュール管理装置の動作と基本的には同様であるので図示を省略する。異なる点は、アクセス権データの代わりに位置情報となるだけである。

【0078】この実施の形態4に係る不正アクセス防止システムは、組織外にある端末1 Aから公衆網2経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置7 Cとアクセスサーバ3 Dを連携させ、ユーザID及びパスワードと、携帯端末1 Aの位置情報とに基づき2重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【0079】実施の形態5. この発明の実施の形態5に係る不正アクセス防止システムについて図面を参照しながら説明する。図14は、この発明の実施の形態5に係る不正アクセス防止システムの構成を示す図である。

【0080】図14において、1 AはGPS機能を有する携帯端末、2は公衆網、3 Eは組織内ネットワークのアクセスサーバ、4は組織内ネットワークのクライアント、6はユーザ毎のユーザIDとパスワードが登録されているファイル装置、7 Dは組織内ネットワークのスケジュール管理装置、8は個人のスケジュールテーブルが登録されているファイル装置である。

【0081】図15は、この発明の実施の形態5に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【0082】図15に示すように、スケジュールテーブルは、ユーザ（個人）毎に構成され、さらに、ユーザー一人について「ユーザ番号」と、「ユーザID」と、時間に対応した「滞在場所」と、同様に時間に対応した「住所（位置情報）」と、同様に時間に対応した「アクセス権（発信元電話番号）」とから構成されている。

【0083】つぎに、この実施の形態5に係る不正アクセス防止システムの動作について図面を参照しながら説明する。図16及び図18は、不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。また、図17は、不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【0084】図15に示すように、ユーザは、行動スケジュールの各項目、すなわち、スケジュールテーブルの「ユーザID」と、一日の時間に対応した「滞在場所」、「住所（位置情報）」及び「アクセス権（発信元電話番号）」をスケジュール管理装置7 Dを介してファイル装置8に登録しておく。スケジュールテーブルで、アクセス権を「禁止」にした時間中は、公衆網2からのアクセスを禁止する。一方、スケジュールテーブルのアクセス権に「電話番号」を登録し、かつスケジュールテーブルの住所（位置情報）に場所を登録すると、その電話番号から、かつ登録した場所からの発信についてのみ公衆網2からのアクセスを許可する。

【0085】上述したように、ユーザは予めスケジュール管理ツールに行動スケジュールを登録しておき、また、GPS機能を備えた携帯端末1 Aを持つ。そして、アクセスサーバ3 Eは、公衆網2からの接続要求を受けた時、使用している携帯端末1 Aの電話番号（発信元電話番号）を公衆網2から受け取る。さらに、GPS機能により認識された「位置情報」を受け取り、「ユーザID」と「発信元電話番号」と「位置情報」をスケジュール管理

ツールへ渡す。

【0086】スケジュール管理ツールでは、受けた「ユーザID」に対応した行動スケジュールを検索し、当該電話番号及び当該位置情報に対応する地域からのアクセスを許可している時間帯かどうかを判定し、アクセスサーバ3Eへ判定結果を返す。この場合の位置情報は、誤差が発生する可能性があるので、必要に応じてアクセスを許可する地域に余裕を持たせる。

【0087】アクセスサーバ3Eでは、スケジュール管理ツールの判定結果が認可であれば携帯端末1Aと組織内ネットワーク間の接続（通信）を、携帯端末1Aからの切断要求を受けるまで保持し、判定結果が否認であれば直ちに通信を切断する。

【0088】すなわち、図16のステップ100において、アクセスサーバ3Eは、携帯端末1Aからアクセス要求を受け付ける。

【0089】次に、ステップ101において、アクセスサーバ3Eは、携帯端末1Aから、「ユーザID」と、「パスワード」と、「発信元電話番号」と、「位置情報」を受け取る。

【0090】次に、ステップ102において、受け取った「ユーザID」及び「パスワード」を、ファイル装置6に登録されているユーザID及びパスワードと比較する。

【0091】次に、ステップ103～104において、携帯端末1Aから受け取った「ユーザID」及び「パスワード」と登録内容が一致した場合は、アクセスサーバ3Eは「ユーザID」、「発信元電話番号」及び「位置情報」をスケジュール管理装置7Bに送る。

【0092】ステップ105～106において、アクセスサーバ3Eは、携帯端末1Aから受け取った「ユーザID」及び「パスワード」と登録内容が一致しなかった場合には、アクセス拒否を携帯端末1Aに通知し、携帯端末1Aとの接続を断つ。

【0093】つづいて、図17のステップ110において、スケジュール管理装置7Dは、「ユーザID」、「発信元電話番号」及び「位置情報」をアクセスサーバ3Cから受け取る。

【0094】次に、ステップ111～112において、スケジュール管理装置7Dは、組織内ネットワーク内の時計から日時を読み込み、「ユーザID」と現在の時間に基づきファイル装置8内のスケジュールテーブルを検索し、登録された発信元電話番号及び位置情報を読み出す。

【0095】次に、ステップ113において、アクセスサーバ3Eから受け取った「発信元電話番号」及び「位置情報」を、ファイル装置8から読み出した発信元電話番号及び位置情報と比較する。

【0096】次に、ステップ114～115において、アクセスサーバ3Eから受け取った「発信元電話番号」及び「位置情報」と登録内容が一致した場合は、スケジュール管理装置7Dはアクセス認可をアクセスサーバ3Eに通知する。

【0097】ステップ116において、スケジュール管理装置7Dは、アクセスサーバ3Eから受け取った「発信元電話番号」及び「位置情報」と登録内容が一致しなかった場合には、アクセス否認をアクセスサーバ3Eに通知する。

【0098】つづいて、図18のステップ120において、アクセスサーバ3Eは、アクセス可否判定結果をスケジュール管理装置7Dから受け取る。

【0099】次に、ステップ121～123において、スケジュール管理装置7Dからアクセス認可を受け取った場合は、アクセスサーバ3Eはアクセス許可を携帯端末1Aに通知し、組織内ネットワークとの通信を許可する。

【0100】ステップ124～125において、アクセスサーバ3Eは、スケジュール管理装置7Dからアクセス否認を受け取った場合には、アクセス拒否を携帯端末1Aに通知し、携帯端末1Aとの接続を断つ。

【0101】この実施の形態5に係る不正アクセス防止システムは、組織外にある端末1Aから公衆網2経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置7Dとアクセスサーバ3Eを連携させ、ユーザID及びパスワードと、携帯端末1Aの電話番号及び位置情報とに基づき2重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【0102】実施の形態6. この発明の実施の形態6に係る不正アクセス防止システムについて説明する。上記の実施の形態5ではスケジュール管理装置7Dで発信元電話番号及び位置情報を登録内容と比較しアクセス可否を判定していたが、この実施の形態6ではアクセスサーバ3Fがアクセス可否の判定を行うものである。

【0103】なお、この実施の形態6に係る不正アクセス防止システムの構成は、上記の実施の形態5とほぼ同様であるので図示を省略する。但し、アクセスサーバ及びスケジュール管理装置の符号を3F及び7Eとする。

【0104】また、この実施の形態6に係る不正アクセス防止システムの動作は、図6～図8に示す実施の形態2のアクセスサーバ及びスケジュール管理装置の動作と基本的には同様であるので図示を省略する。異なる点は、アクセス権データに位置情報が加えられているだけである。

【0105】この実施の形態6に係る不正アクセス防止システムは、組織外にある端末1Aから公衆網2経由で組織内ネットワークへ接続する場合に、個人の行動スケジュールを管理するスケジュール管理装置7Eとアクセスサーバ3Fを連携させ、ユーザID及びパスワードと、携帯端末1Aの電話番号及び位置情報とに基づき2重に接続可否を判定することにより、セキュリティの強化を図ることができる。

【0106】

【発明の効果】この発明に係る不正アクセス防止システムは、以上説明したとおり、携帯端末からアクセス要求があった場合には前記携帯端末からユーザID及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザID及び第1のユーザ識別情報を受け取り前記第1のユーザ識別情報とスケジュールテーブルに予め登録された

第2のユーザ識別情報と比較してその結果を前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザID、パスワード及び第1のユーザ識別情報を受け取り前記ユーザID及びパスワードと登録内容と比較して一致したときは前記ユーザID及び第1のユーザ識別情報を前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記比較結果を受け取り前記第1及び第2のユーザ識別情報が一致しているときはアクセス許可を前記携帯端末に通知し、一致していないときにはアクセス拒否を前記携帯端末に通知するので、2重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【0107】この発明に係る不正アクセス防止システムは、以上説明したとおり、携帯端末からアクセス要求があった場合には前記携帯端末からユーザID及びパスワードを受け取り登録内容と比較して一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するアクセスサーバを備えた不正アクセス防止システムにおいて、さらに、前記アクセスサーバからユーザIDを受け取り前記ユーザIDに基づきスケジュールテーブルから予め登録された第2のユーザ識別情報を読み出して前記アクセスサーバに通知するスケジュール管理装置を備え、前記アクセスサーバは、前記携帯端末からアクセス要求があった場合には前記携帯端末からユーザID、パスワード及び第1のユーザ識別情報を受け取り前記ユーザID及びパスワードと登録内容と比較して一致したときは前記ユーザIDを前記スケジュール管理装置に渡し、また、前記アクセスサーバは、前記スケジュール管理装置から前記第2のユーザ識別情報を受け取り前記第1及び第2のユーザ識別情報が一致したときはアクセス許可を前記携帯端末に通知し、一致しないときにはアクセス拒否を前記携帯端末に通知するので、2重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【0108】また、この発明に係る不正アクセス防止システムは、以上説明したとおり、前記第1及び第2のユーザ識別情報を、前記携帯端末の発信元電話番号としたので、2重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【0109】また、この発明に係る不正アクセス防止システムは、以上説明したとおり、前記第1のユーザ識別情報を、前記携帯端末の位置情報とし、前記第2のユーザ識別情報を、前記登録された位置情報としたので、2重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。

【0110】さらに、この発明に係る不正アクセス防止システムは、以上説明したとおり、前記第1のユーザ識別情報を、前記携帯端末の発信元電話番号及び位置情報とし、前記第2のユーザ識別情報を、前記携帯端末の発信元電話番号及び前記登録された位置情報としたので、2重に接続可否を判定することになり、セキュリティの強化を図ることができるという効果を奏する。



## 図の説明

---

### 【図面の簡単な説明】

【図 1】 この発明の実施の形態 1 に係る不正アクセス防止システムの構成を示す図である。

【図 2】 この発明の実施の形態 1 に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【図 3】 この発明の実施の形態 1 に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図 4】 この発明の実施の形態 1 に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図 5】 この発明の実施の形態 1 に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図 6】 この発明の実施の形態 2 に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図 7】 この発明の実施の形態 2 に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図 8】 この発明の実施の形態 2 に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図 9】 この発明の実施の形態 3 に係る不正アクセス防止システムの構成を示す図である。

【図 10】 この発明の実施の形態 3 に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【図 11】 この発明の実施の形態 3 に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図 12】 この発明の実施の形態 3 に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図 13】 この発明の実施の形態 3 に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図 14】 この発明の実施の形態 5 に係る不正アクセス防止システムの構成を示す図である。

【図 15】 この発明の実施の形態 5 に係る不正アクセス防止システムのスケジュールテーブルの構成を示す図である。

【図 16】 この発明の実施の形態 5 に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

【図 17】 この発明の実施の形態 5 に係る不正アクセス防止システムのスケジュール管理装置の動作を示すフローチャートである。

【図18】 この発明の実施の形態5に係る不正アクセス防止システムのアクセスサーバの動作を示すフローチャートである。

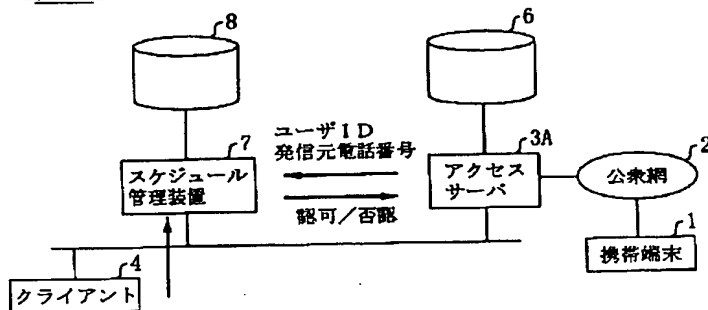
【図19】 従来の不正アクセス防止システムの構成を示す図である。

【符号の説明】

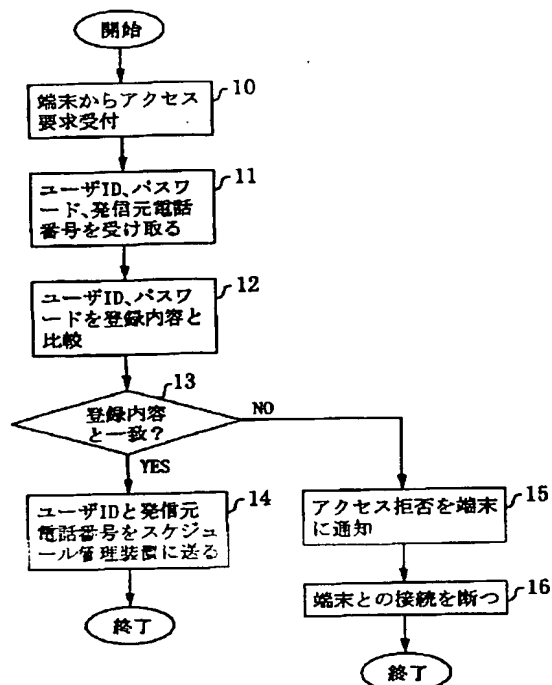
1 携帯端末、1A GPS機能を備えた携帯端末、2 公衆網、3A、3B、3C、3D、3E、3F アクセスサーバ、4 クライアント、6 ファイル装置、7、7A、7B、7C、7D、7E スケジュール管理装置、8 ファイル装置。

図面

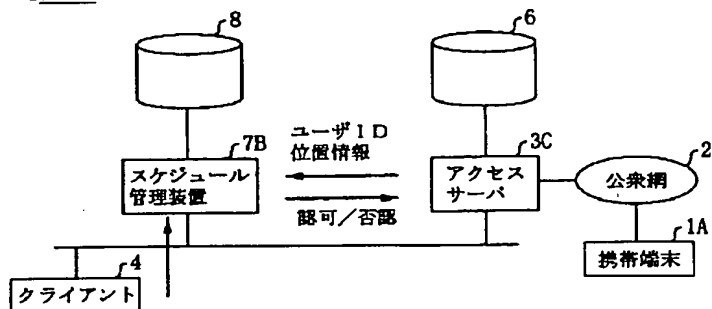
【図1】



【図3】



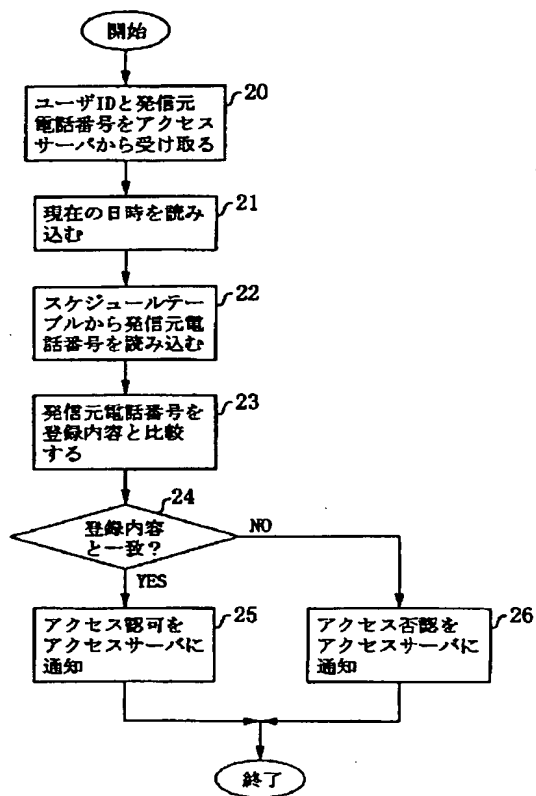
【図9】



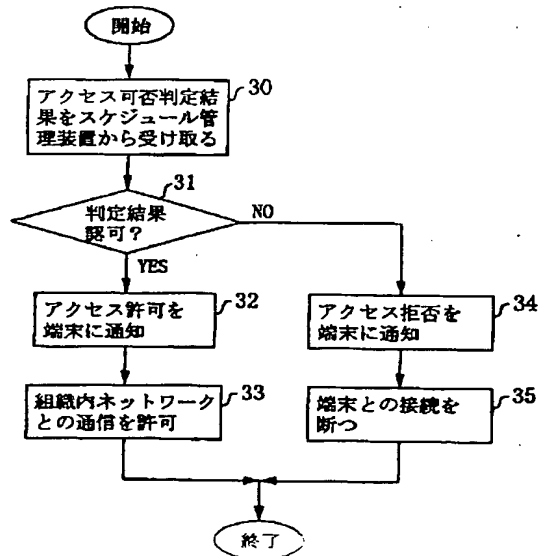
【図2】

ユーザ 番号	ユーザ ID	時間	... 9 10 11 12 13 14 15 16 17 18 19 20 ...															
1	user1	滞在場所	～	構内			移動		X大学			移動		自宅				
		アクセス権 (発信元 電話番号)	～	禁止			030-XX-XXXX		030-XX-XXXX			030-XX-XXXX		030-XX-XXXX				
2	user2	滞在場所	～	構内		移動	Y社		移動	Z事業所		移動	自宅					
		アクセス権 (発信元 電話番号)	～	禁止		030-XX-XXXX	030-XX-XXXX	030-XX-XXXX	030-XX-XXXX	030-XX-XXXX	045-XX-XXXX	045-XX-XXXX						
3	user3	滞在場所	自宅															
		アクセス権 (発信元 電話番号)	03-XXXX-XXXX															
}	}	}	}															

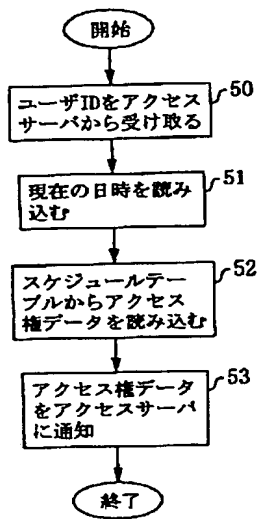
【図4】



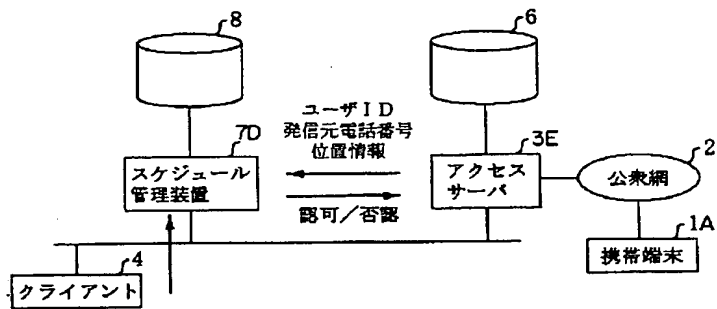
【図5】



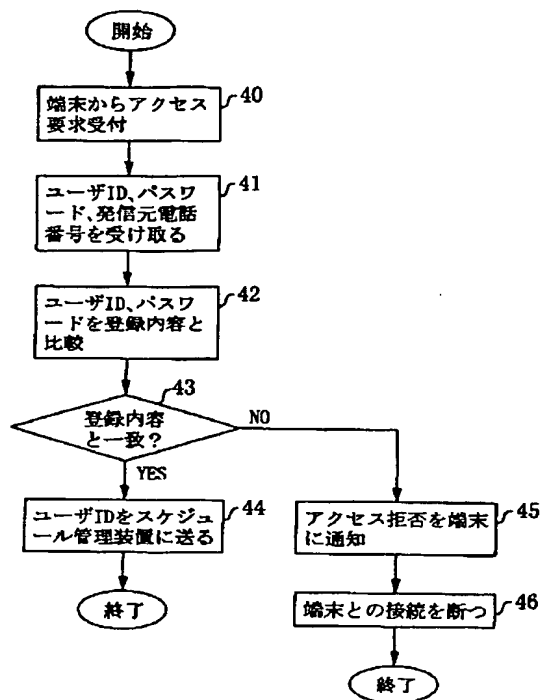
【図7】



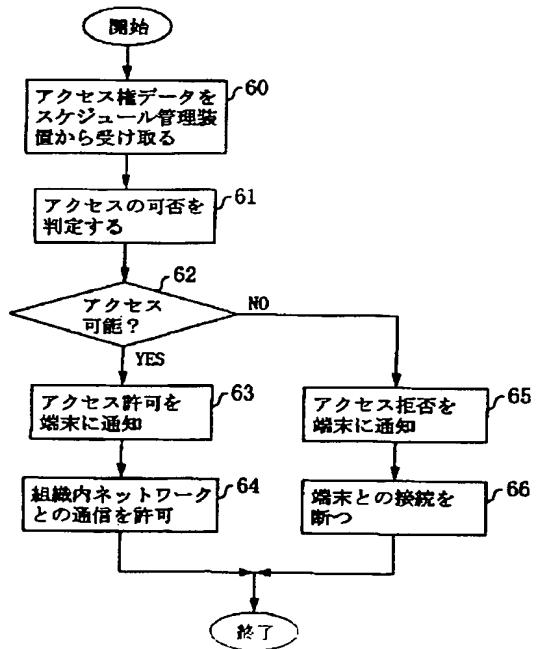
【図14】



【図6】



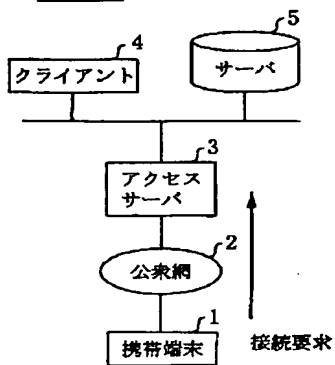
【図 8】



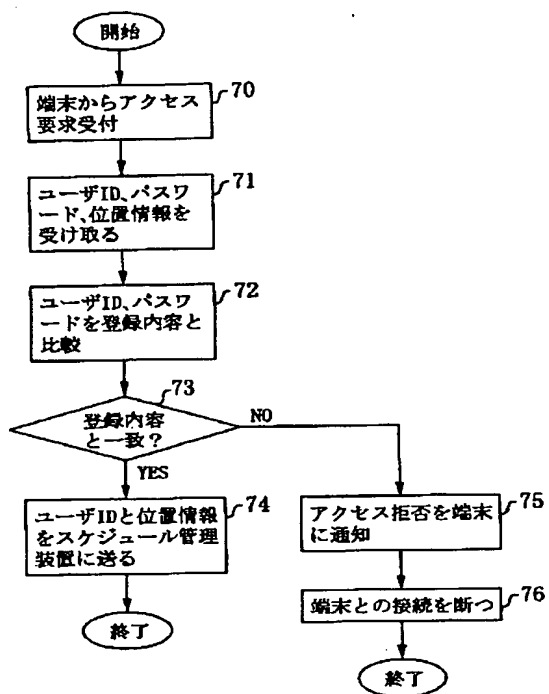
【図 10】

ユーザ 番号	ユーザ ID	時間	... 9 10 11 12 13 14 15 16 17 18 19 20 ...																	
			滞在場所	～	構内		移動		X大学		移動		自宅							
1	user1	住所 (位置情報)	～	A市K区		A市、 B市		B市L町		B市、 C市		C市M区								
		滞在場所	～	構内	移動	Y社		移動	Z事業所		移動	自宅								
2	user2	住所 (位置情報)	～	A市K区	A市、 D市	D市N町		D市	D市O町	D市、 E市	E市P町									
		滞在場所	自宅																	
3	user3	住所 (位置情報)	A市Q区																	
		滞在場所																		
}	}	}	}																	

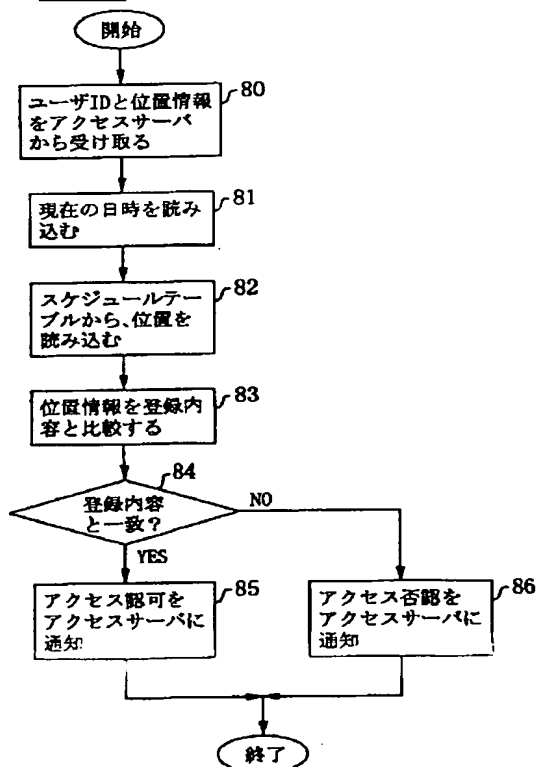
【図19】



【図11】

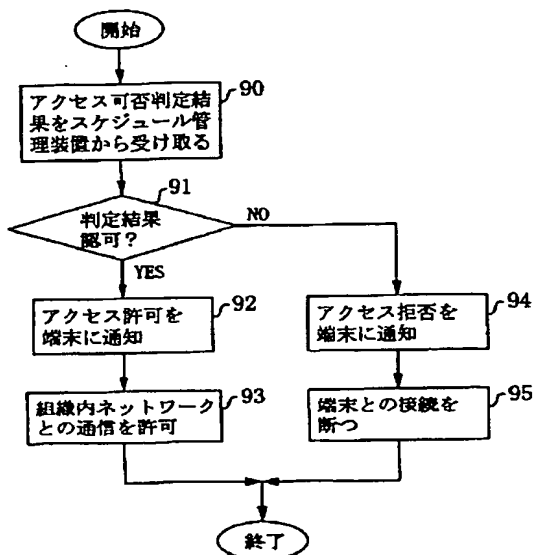


【図12】

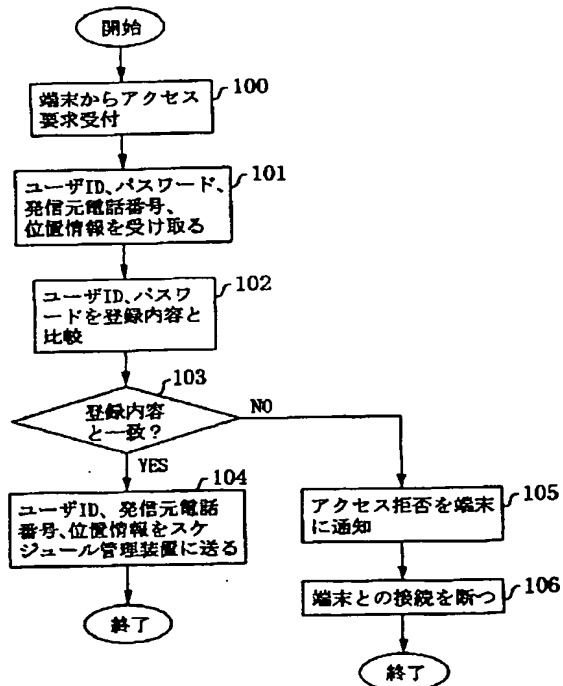




【図13】



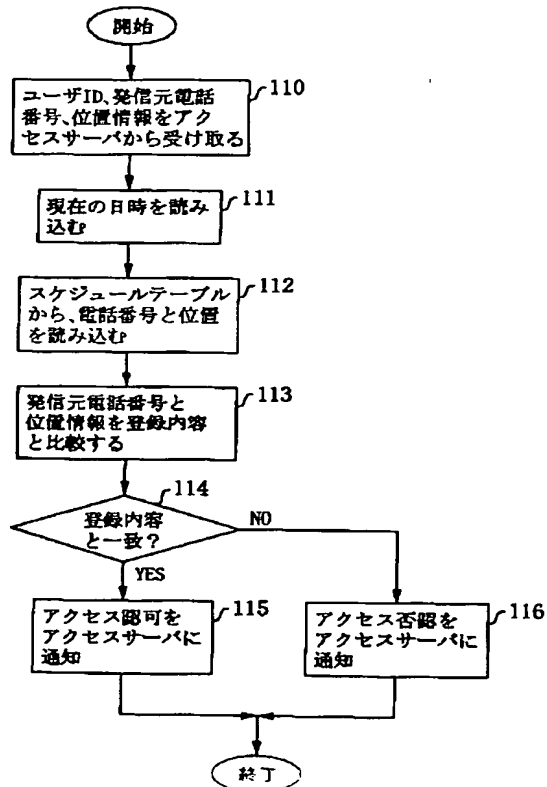
【図16】



【図15】

ユーザ 番号	ユーザ ID	時間	... 9 10 11 12 13 14 15 16 17 18 19 20 ...													
1	user1	滞在場所	～	構内			移動		X大学			移動		自宅		
		住所 (位置情報)	～	A市K区			A市、B市		B市L町			B市、C市		C市M区		
		アクセス権 (発信元 電話番号)	～	禁止			030-XX-XXXX		030-XX-XXXX			030-XX-XXXX		030-XX-XXXX		
2	user2	滞在場所	～	構内	移動		Y社		移動		Z事業所		移動		自宅	
		住所 (位置情報)	～	A市K区	A市、D市	D市N町		D市		D市O町		D市、E市		E市P町		
		アクセス権 (発信元 電話番号)	～	禁止	030-XX-XXXX	030-XX-XXXX		030-XX-XXXX		030-XX-XXXX		030-XX-XXXX		045-XX-XXXX		
3	user3	滞在場所	自宅													
		住所 (位置情報)	A市Q区													
		アクセス権 (発信元 電話番号)	03-XXXX-XXXX													
?	?	?	?													

【図17】



【図18】

